BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

M.D., O.F., and J.P., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC and META PLATFORMS, INC.,

Defendants.

Case No. 3:24-cv-06369-AMO

PLAINTIFFS' OPPOSITION TO DEFENDANT GOOGLE LLC'S MOTION TO DISMISS FIRST AMENDED CLASS ACTION COMPLAINT

Hearing: July 10, 2025
Time: 2:00 p.m.
Location: Courtroom 10—19th Floor
Judge: Hon. Araceli Martínez-Olguín

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

REGULATIONS

I. INTRODUCTION

The "free" advertising tools Defendant Google LLC ("Defendant" or "Google") offers to website operators come with a troubling cost for consumers. Instead of charging website operators like Dermacare LLC d/b/a BlueChew ("BlueChew") for the use of its tools, Google demands something more valuable: protected health data. Blue Chew operates a website where consumers can qualify for and purchase prescription erectile dysfunction mediation. When companies like BlueChew install Google's tracking technologies onto their websites, Google knows that it will inevitably collect protected health data from consumers. That is by design. At its core, Google is an advertising company. It is one of the most profitable advertising companies in the world. While certain Google tools such as Google Analytics do provide analytical services for Google's customers, like BlueChew, Google Analytics is a foundational part of Google's advertising services. That is because all data collected through Google Analytics, including data that is legally protected, is fed into Google's advertising machinery. Google knows it collects data that is inherently unlawful for it to possess but chooses to feign ignorance (as it does here) due to the value the data possesses. Plaintiffs M.D., O.F., and J.P. (collectively "Plaintiffs") bring this action to stop Google's unlawful practices.

Plaintiffs hereby oppose Defendant's Motion to Dismiss the First Amended Class Action Complaint (ECF No. 40) ("MTD"). Plaintiff M.D. plausibly states a claim under the California Invasion of Privacy Act ("CIPA") § 631(a) and § 632 and for invasion of privacy because Defendant intentionally, and without the consent of Plaintiffs and class members, intercepted sensitive and confidential health communications between Plaintiffs (and class members) and third party BlueChew, via the BlueChew website, www.bluechew.com (the "Website"). Plaintiff O.F. states a claim under the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et seq.* ("WESCA") based on the same conduct. Plaintiff J.P. states a claim under the Maryland Wiretapping and Electronic Surveillance Act, Md. Code, Cts. & Jud. Proc. Code Sec. 10-401, *et seq*. ("MWESA") based on the same conduct.

BlueChew is an online health platform wherein registered users connect with health care providers for the diagnosis and treatment of erectile dysfunction. Through the Website, users, such

as Plaintiffs and class members, fill out a medical questionnaire and, if they qualify, purchase erectile dysfunction medication. While Plaintiffs and class members reasonably believed and expected that their communications with BlueChew regarding these sensitive health issues would be kept confidential, they were not. That is because BlueChew embedded Defendant's software on its Website, Google Analytics, which captured Plaintiffs' and class members' interactions with the Website—including their personal information and information regarding the erectile dysfunction medications they purchased—and transmitted said health information to Defendant. Defendant then used this information for its own benefit by incorporating it into its advertising machinery which functioned to place Plaintiffs and class members into targeted audiences for advertisers of similar medications. Indeed, Plaintiffs in this case were retargeted and subject to advertising for erectile dysfunction medications because of Defendant's use of their confidential health information. Defendant makes its tracking technologies free for website owners to use for exactly that reason, so that it can receive information from website interactions and then generate highly specific audience segments which it then uses to sell advertising. However, where, as here, protected health information is surreptitiously transmitted to Defendant without the consent of Plaintiffs and class members, it is unlawful.

As a result of Defendant's unlawful conduct, Plaintiff M.D. brings the present action on behalf of himself and "all natural persons in California who, during the class period, purchased medication on www.bluechew.com." *See* First Amended Class Action Complaint (ECF No. 34) ("FAC"), ¶ 78. Plaintiff O.F. brings claims on behalf of himself and an identical class of persons in Pennsylvania. *Id.* ¶ 79. Plaintiff J.P. brings claims on behalf of himself and an identical class of persons in Maryland. *Id.* ¶ 80.

Defendant now moves to dismiss Plaintiffs' claims. However, courts have rejected similar motions to dismiss in other cases involving similar tracking technologies. *See Smith v. Google, LLC*, 735 F. Supp. 3d 1188 (N.D. Cal. 2024); *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. 2021); *Doe, et al. v. GoodRx Holdings, Inc., et al.*, Case No. 3:23-cv-00501-AMO (N.D. Cal.). For the reasons set forth herein, the Court should deny Defendant's motion to dismiss.

II. STATEMENT OF FACTS

BlueChew's Website allows registered users to connect with health care providers for the diagnosis and treatment of erectile dysfunction. FAC ¶ 2; ¶¶ 19-20, Figure 1. The Website offers patients discrete access to prescription erectile dysfunction medications. *Id.* In using the Website, Plaintiffs and class members provided protected health information to BlueChew for the purpose of obtaining medical treatment, including providing responses to a "medical profile" questionnaire to determine whether they qualify for erectile dysfunction medication. *Id.* ¶¶ 20-24, Figures 1-4. Based on the questionnaire responses, Plaintiffs and class members purchased erectile dysfunction medications. *Id.*

Despite being protected by federal and state law, and unbeknownst to Plaintiffs and Class Members, Defendant intercepted their sensitive health information conveyed through the Website using its Google Analytics tool, and other similar software. The data intercepted and collected included de-anonymized prescribed medications purchased by Plaintiffs and class members on the Website. *Id.* ¶¶ 61-75 (illustrating how Google's tracking technologies function to intercept private health information from the Website). Plaintiffs' protected health information that Defendant intercepted was personally identifiable and Defendant used Plaintiffs' and class members' intercepted health information for its own benefit, namely, for the purpose of targeted advertising. *Id.* ¶¶ 5, 73-74. Examples of Defendant's interceptions from the Website show that Defendant intercepted personally identifying information such as name, state of residence, email address, and various forms of protected health information. For example, Defendant intercepted information showing that the BlueChew user registered on the Website, added a medication to their cart, and ultimately purchased the medication. *Id.* ¶ 67-69, Figures 8 and 9. Regardless of whether Plaintiffs and class members hold accounts with Google, Defendant can match their prescription information to their identity using the personally identifying information they conveyed to BlueChew that was intercepted by Defendant. *Id.*

At no point during the checkout process on the Website were Plaintiffs and class members alerted that information related to their prescription medications was being intercepted by Defendant. *Id.* ¶ 25. At all relevant times, Plaintiffs and class members had a reasonable expectation of privacy

as to the protected health information they transmitted to BueChew because they reasonably believed the communications were between them and BlueChew, and they did not consent to Defendant's interception of their private health information. *Id.* ¶ 6; *see also id.* ¶ 13 (Defendant "committed the interceptions at issue without Plaintiffs' knowledge, consent, or express written authorization.").

Plaintiff M.D. is a California citizen who, on December 6, 2022, and January 4, 2023, was prescribed and ordered Sildenafil erectile dysfunction medication through the Website. *Id.* ¶ 7. Unbeknownst to Plaintiff M.D., Defendant intercepted his protected health information related to his prescription medication using the Facebook Tracking Pixel. *Id.* In addition to information related to his prescription medication, Defendant also intercepted Plaintiff M.D.'s personally identifiable information, including his first and last name, email address, and date of birth. *Id.* ¶ 8. Subsequently, because of Defendant's conduct, Plaintiff M.D. has received targeted advertisements relating to erectile dysfunction medications. *Id.* Plaintiff O.F., a Pennsylvania citizen, and Plaintiff J.P., a Maryland citizen, make identical allegations to those of Plaintiff M.D. *Id.* ¶¶ 9-12. Plaintiffs did not discover Defendant's surreptitious interception of their personal health information until September 2024. *Id.* ¶¶ 7, 9, 11. For its part, Defendant knew that the incorporation of its software onto the Website would result in its interception of protected health information and personally identifying information of Plaintiffs and class members. *Id.* ¶ 14. As demonstrated by the continued incorporation of the Google tracking technologies on the Website, Defendant intends to intercept this protected and sensitive health data due to the value it holds for targeted advertising. *Id.* ¶ 94.

III. ARGUMENT

A. Plaintiffs Did Not Consent To Google's Collection Of Their Private Health Information

Defendant argues that Plaintiffs' state wiretapping claims fail because they "consented to BlueChew's Privacy Policy, which disclosed the Website's use of Google Analytics[.]" MTD at 8. That is wrong. Defendant's reliance on cherry-picked language from BlueChew's privacy policy is insufficient to establish consent for the interceptions at issue here.

"On a motion to dismiss, the burden of proof to show consent rests with defendants." *Doe v. FullStory, Inc.*, 712 F. Supp. 3d 1244, 1253 (N.D. Cal. 2024); *Doe v. Meta Platforms, Inc.*, 690 F.

Supp. 3d 1064, 1077–78 (N.D. Cal. 2023) ("On this motion to dismiss, the issue of consent is front and center and the burden of proof to show this exemption applies is on Meta."); *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) ("Google next claims there was lawful consent from both the account holder and the websites. Google bears the burden of proof on consent."). Here, Plaintiffs allege they did not consent to Defendant's interception of their confidential health information conveyed to BlueChew. FAC ¶ 6; *see also id.* ¶ 13 (Defendant "committed the interceptions at issue without Plaintiffs' knowledge, consent, or express written authorization."), *id.* ¶ 93. Nevertheless, Defendant argues that Plaintiffs consented based on BlueChew's Privacy Policy.

Before addressing the substance of the purported Privacy Policy, there are several issues that prevent dismissal. First, Plaintiffs do not reference the BlueChew Privacy Policy in the FAC and specifically allege that at "no point during the checkout process are patients alerted that information related to their prescription medication is being intercepted by third parties." FAC ¶ 25. As such, Defendant's argument, which improperly relies on documents extraneous to the pleadings, is belied by Plaintiffs' allegations. *Smith*, 735 F. Supp. 3d at 1196 ("Although these documents suggest that plaintiffs *could* have consented to Google's alleged data collection, plaintiffs specifically allege that they did not. The mere existence of various terms of service and privacy policies cannot establish at this stage, where the Court must draw all reasonable inferences in plaintiffs' favor, that any of the plaintiffs *did* in fact consent. Google's consent arguments do not provide a basis to dismiss the Section 631 claim."). Even if considered by the Court, what a reasonable consumer would believe if they were on notice of the privacy statements at issue cannot be determined at this stage, without any discovery. *See*, *e.g.*, *Fan v. NBA Properties Inc.*, 2024 WL 1297643, at *3 (N.D. Cal. Mar. 26, 2024) ("[w]hether reasonable consumers would understand, based on the … Terms of Use or … Privacy Policy, that by using the … website they were consenting to the disclosure of their personally identifiable information … is a question that should be resolved on a fuller factual record."); *Hilfiker Square, LLC v. Thrifty Payless, Inc.*, 2016 WL 7031283, at *3 (D. Or. Nov. 29, 2016) ("dismissal at this stage in the proceedings is inappropriate, especially because a determination regarding the parties' objectively reasonable expectations generally involves a question of fact"); *Turner v. Nuance*

Commc'ns, Inc., 735 F. Supp. 3d 1169 (N.D. Cal. 2024) (declining to dismiss CIPA claim based on consent where "there is a factual dispute over whether the DAA sufficiently notified Plaintiffs of Nuance's conduct"); *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *6 (N.D. Cal. Feb. 2, 2021) ("At the motion to dismiss stage, the Court is not prepared to rule that the Privacy Policy establishes an absolute bar to Plaintiff's claims."); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1078 (N.D. Cal. 2023) ("Determination of whether actual consent was given depends on what Meta disclosed to healthcare providers, how it described and trained healthcare providers on the Pixel, and how the healthcare providers understood the Pixel worked and the information that then could or would be collected by Meta.").

In any event, BlueChew's purported Privacy Policy does not establish consent because it did not "explicitly notify" Plaintiffs of the practice at issue. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) ("In order for consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue."); *In re Google Inc.*, 2013 WL 5423918, at *13 (N.D. Cal. Sept. 26, 2013) ("Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising."); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) ("However, as discussed above in the context of express consent, any consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case—that is, the scanning of message content for use in targeted advertising.").

In fact, BlueChew's Privacy Policy states the *opposite*, that it safeguards sensitive health information and only shares it with certain enumerated third parties for certain purposes which do not include online advertising. For example, the Privacy Policy states:

> **Personally Identifiable Information**
> BLUECHEW may share information about you, including health information and other information that personally identifies you, as follows:

- with healthcare providers with whom you are connected via BLUECHEW for the provision of their healthcare services to you;
- with pharmacies, to fulfill prescriptions from your healthcare providers and coordinate medication orders;
- with service providers that we use to support the Websites or otherwise in connection with administering and providing our Services, and billing and collections, including without limitation any third party payment processor;
- with other third parties as we deem appropriate or necessary to comply with applicable laws or legal process, such as in response to a subpoena in compliance with applicable privacy laws, or to enforce our Terms and Conditions;
- to a buyer or successor in the event of a sale, merger or other transaction that involves the transfer of such information to the other company.

RJN, Ex. 5-C p.2. None of these enumerated scenarios remotely disclose the conduct at issue here. The law requires explicit notification, not attenuated, unsupported suppositions Defendant makes. The BlueChew Privacy Policy falls far short of providing explicit notification of the conduct at issue. This is bolstered by the fact that, in the very section relied upon by Defendant (USE OF COOKIES AND OTHER TECHNOLOGIES ON THE WEBSITES), the Privacy Policy also explicitly states: "[w]e do not share your personal information with these third parties [i.e., Google]." *Id.* at 4. Indeed, the conduct alleged here is directly contrary to the representations in the Privacy Policy.

The purported March 29, 2023 Privacy Policy does not change the analysis because there is still no explicit notification by BlueChew that it will share health information with Google. Instead, this iteration of the privacy policy still explicitly warrants the opposite. *See* RJN, Ex. 5-E at 2. ("We do not share your personal information with these third parties [i.e. Google]." As such, Defendant fails to demonstrate that any Plaintiff consented to the conduct at issue here at any time.

B. Plaintiffs Adequately Allege Intent

Defendant argues that Plaintiffs' state wiretapping claims should be dismissed because they "cannot plausibly allege that Google *intended* to receive PII or PHI." MTD at 11. That is wrong.

Analyzing intent under CIPA involves a similar analysis to the federal Wiretap Act. *M.G. v. Therapymatch, Inc.*, 2024 WL 4219992, at *3 (N.D. Cal. Sept. 16, 2024) (Martínez-Olguín, J.) ("The analysis for a violation of CIPA is the same analysis for a violation of the federal Wiretap Act."); *see*

also Brodsky v. Apple Inc., 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020); *Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041, at *4 (N.D. Cal. Dec. 30, 2024). For CIPA § 632(a), the statute punishes "a person who intends to make a recording of a confidential communication." *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 435 (2018) (internal quotation marks and citation omitted). The standard under MWESA is similar to CIPA, as the "willfulness *mens rea* does not require a showing of 'bad motive' or 'knowing unlawfulness'"; instead, "[i]t is sufficient to show that there was an intentional, rather than inadvertent or negligent, interception." *Holmes v. State*, 236 Md. App. 636, 649 (2018) (quoting *Deibler v. State*, 365 Md. 185, 199 (2001)). Similarly, "WESCA is Pennsylvania's state law equivalent to the Federal Wiretap Act." *Ingrao v. AddShoppers, Inc.*, 2024 WL 4892514, at *12 (E.D. Pa. Nov. 25, 2024); *see also Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125–26 (3d Cir. 2022) (WESCA "operates in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, which provides uniform minimum protections for wire, electronic, or oral communications."). Therefore, the intent analysis under CIPA, MWESA, and WESCA is the same.

As a threshold matter, "[w]hether a person possesses the requisite intent under CIPA is generally a question of fact." *Gladstone v. Amazon Web Servs., Inc.*, 739 F. Supp. 3d 846, 859 (W.D. Wash. 2024); *see also Smith v. Google, LLC*, 735 F. Supp. 3d 1188, 1198 (N.D. Cal. 2024) ("While Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited developers from transmitting such data, this presents a question of fact that the Court cannot resolve at this stage."); *Hudson v. Superior Ct.*, 7 Cal. App. 5th 1165, 1171 (2017) ("[A] person's intent is a question of fact to be determined from all the circumstances of the case, and usually must be proven circumstantially." (internal citations omitted)). Pennsylvania courts have reached the same conclusion. *United States v. Fumo*, 628 F. Supp. 2d 573, 592 (E.D. Pa. 2007) ("Intent is a question of fact, to be determined by a jury."). Additionally, "interceptions may be considered intentional where a defendant is aware of the defect causing interception and takes no remedial action." *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020); *see also Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014) (collecting cases).

Here, Plaintiffs adequately allege knowledge and intent under each applicable cause of action. *See* FAC ¶¶ 5, 14, 94, 96, 115, 125-26, 137. Plaintiffs allege that Google Analytics is designed for the purpose of recording and analyzing communications between Defendant's customers (like BlueChew) and consumers (like Plaintiffs and class members). *Id.* ¶¶ 59-75; *see also Gladstone*, 739 F. Supp. 3d at 860 (finding intent element under CIPA § 631(a) and § 632(a) satisfied where "[t]he SAC alleges that Amazon Connect is designed for the purpose of recording and analyzing communications between its customers (like Capital One) and consumers or other entities"). Defendant also knew that Google Analytics may intercept "sensitive" data as evidenced by its own internal policies, which specifically acknowledges that the Google Analytics could be configured to share "health" information with Google. *See* MTD at 13. Defendant's knowledge is also gleaned from its involvement in other litigations in which its tracking technologies, including Google Analytics, have been used to intercept and transmit to Defendant sensitive information. *See Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. Mar. 12, 2021); *Smith*, 735 F. Supp. 3d 1188; *Calhoun v. Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. Mar. 17, 2021); *Doe, et al. v. GoodRx Holdings, Inc., et al.*, Case No. 3:23-cv-00501-AMO (N.D. Cal.).

Defendant is aware that the information it intercepts on health websites, like the Website here, contains legally protected information. Despite the repeated instances of intercepting legally protected information without authorization or consent, Defendant has failed to take remedial action to prevent sensitive health information from being transmitted to it via its tracking technologies, including in this case. Defendant has also failed to destroy the protected health information it received from Plaintiffs, evidencing intent. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 827–28 ("[T]he Court finds that Defendants' failure to rectify the defect causing 'false accepts' or destroy the recordings produced under such circumstances could plausibly be considered 'intentional' rather than 'a result of accident or mistake.'"). On the contrary, Defendant has affirmatively *used* the protected health information it intercepted via Google Analytics to improve its advertising machinery and generate revenue. FAC ¶¶ 5, 73-74. Indeed, Plaintiffs were targeted with similar advertisements promoting erectile dysfunction medications after visiting the Website. *Id.* ¶¶ 8, 10, 12. In short, Defendant's interception of Plaintiffs' and class members' confidential

health information was no accident, it was intended by Defendant. Otherwise, Defendant would not have used the intercepted confidential information to power its own algorithms and advertising products to derive a profit. *Id.* ¶¶ 5, 73-74.

Defendant further argues that its Terms of Service exonerate it from liability. MTD at 13. But identical argument have been squarely rejected in other similar cases. In *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064 (N.D. Cal. 2023) ("*Meta*"), *motion to certify appeal denied*, 2024 WL 4375776 (N.D. Cal. Oct. 2, 2024), the court found:

> While plaintiffs acknowledge that Meta may tell third parties and Facebook users that it intends to prevent receipt of sensitive health information, plaintiffs contend that is not what Meta really intends. . . What Meta's true intent is, what steps it actually took to prevent receipt of health information, the efficacy of its filtering tools, and the technological feasibility of implementing other measures to prevent the transfer of health information, all turn on disputed questions of fact that need development on a full evidentiary record. . . At this stage, intent has been adequately alleged.

Id. at 1076.

The same analysis applies here. The point is not that Google's terms exist, the point is that Defendant acts contrary to its stated position by collecting sensitive data by the means set forth above. *See In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 1003 (N.D. Cal. 2024) ("Meta argues that it could not have intended to receive the information at issue because its Business Tools Terms forbid developers from sending sensitive information to Meta and require that developers have all necessary rights and permissions to lawfully share whatever information they send. . . [T]he Court cannot conclude from their mere existence that Meta and developers intended to or did comply with the terms rather than deviating from them to their mutual benefit."). Defendant's intent is, at best, a question of fact. *Id.*; *Gladstone*, 739 F. Supp. 3d at 860 ("Defendant points out that it contractually requires companies that use Amazon Connect to provide notice and obtain consent from their customers . . . but the Court is not convinced that [Defendant's] inclusion of a catch-all provision requiring its customers to comply with the law generally is enough to satisfy its legal obligations under CIPA.") (cleaned up).

Defendant further argues that it was "BlueChew [that] shared data with Google[.]" MTD at 12. But as stated above, Defendant obtained and used the intercepted health information for its own benefit, which strongly evidences intent. FAC ¶¶ 5, 73-74.

Defendant cites to *Doe I v. Google LLC*, 741 F. Supp. 3d 828, 836 (N.D. Cal. 2024) ("*Google*"), wherein the court granted a motion to dismiss because the plaintiffs' allegations were "too vague to support an inference that the providers have, contrary to [Google's] admonition [not to use the pixel to transmit health information], caused Google to receive the plaintiffs' personal health information" and that the plaintiffs did not "adequately allege that Google intends to receive this information, or that Google intends to feed the information into its own advertising machinery." *Id.* at 836. But numerous other cases in this District have correctly departed from the reasoning in *Google* with regard to Google's tracking technologies. *See Smith*, 735 F. Supp. 3d at 1198 ("While Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited developers from transmitting such data, this presents a question of fact that the Court cannot resolve at this stage."); *Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234, at *11 (N.D. Cal. Aug. 22, 2023) (finding intent met with regard to implementation of the Facebook Tracking Pixel and rejecting many of the same arguments raised by Defendant here).

The weight of existing authority favors Judge Orrick's analysis in *Meta*, which this Court should apply here. Even if this Court were to decline to follow the factually analogous cases involving the same technology (*Smith* and *Gershzon*), and instead follow the decision in *Google*, it is distinguishable. Unlike in *Google*, where there was no allegation that "Google intends to feed the information into its own advertising machinery," here, Plaintiffs allege that Defendant knowingly receives the confidential health information from BlueChew and integrates it into its proprietary advertising products. FAC ¶¶ 5, 73-74.

Finally, Defendant's argument regarding the appropriate standard of review regarding Plaintiff's wiretapping allegations has already been rejected. *See Smith*, 735 F. Supp. 3d at 1198 (finding that "Plaintiffs' statutory claims here do not sound in fraud. Their claim requires intent,

which plaintiffs have specifically alleged. That Google also allegedly misrepresented its true intent is a separate issue from whether Google actually did intend to receive the data.").

C. Plaintiffs' Communications With Their Healthcare Provider Were Confidential

Defendant argues that Plaintiffs' communications were not confidential in the context of their state law wiretapping claims for three reasons: (1) Plaintiffs consented to the use of Google Analytics, (2) there is a presumption that internet-based communications are not confidential, and (3) that there was no meaningful way for Google to know the meaning of the "pseudonymous identifier" it intercepted. *See* MTD at 15-18. Defendant is wrong on all counts.

First, Defendant's recycled argument that Plaintiffs consented to the use of Google Analytics is directly contradicted by BlueChew's Privacy Policies. Indeed, as discussed *supra*, BlueChew's Privacy Policies specifically warrant that "[w]e do not share your personal information with these third parties [i.e., Google]." RJN, Ex. 5-C at 4. Therefore, Plaintiffs did not consent to any PII and PHI being intercepted and recorded by Google. *See Calhoun*, 526 F. Supp. 3d at 620 (N.D. Cal. 2021); *In re Google Inc.*, 2013 WL 5423918, at *13.

Second, there is no presumption that internet-based communications are not confidential. *See Brown v. Google LLC*, 685 F. Supp. 3d 909, 938 (N.D. Cal. 2023) ("California courts have never recognized a legal 'presumption' that internet communications are not confidential under Section632."); *Smith*, 735 F. Supp. 3d at 1199 (same). A communication is confidential under Section 632 if a party "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 41 P. 3d 575, 582 (Cal. 2002); *Brown*, 685 F. Supp. 3d at 939. Whether a plaintiff had an objectively reasonable expectation that her confidential communications were not being recorded often presents factual issues not appropriately resolved at the pleading stage. *See Lieberman v. KCOP Television, Inc.*, 110 Cal.App.4th 156, 169, 1 Cal.Rptr.3d 536 (2003) ("It is for the jury to decide whether under the circumstances presented [plaintiff] could have *reasonably* expected that the communications were private."); *Brown*, 685 F. Supp. 3d at 937 (finding confidentiality under Section 632 to be "a fact-intensive inquiry" not appropriately resolved at summary judgment). Here, Plaintiffs possessed an objectively reasonable expectation that their

PII and PHI associated with their purchase of prescription erectile dysfunction medication was not being recorded. Defendant has failed to produce any evidence that Plaintiffs would have been aware that the sensitive aspects of their communications with their healthcare provider were being recorded by a third party for advertising purposes.

Third, Defendant's assertion that a "pseudonymous identifier," "is unintelligible, and is not fairly characterized as medical information," contradicts both Plaintiffs' allegations and relevant case law. MTD at 18. As conceded by Defendant, "Each of BlueChew's medications are assigned their own unique content ID. These unique IDs indicate the type of medication being purchased by patients, as well as the quantity and dosage. For example, the content ID "1" indicates that a patient has selected a 6-pack of BlueChew's 30 mg Sildenafil prescription medication. Similar unique IDs are used for all varieties of BlueChew's prescriptions. Based on these unique IDs, [Google] possesses information about the prescription medication being purchased by BlueChew's patients." FAC ¶ 44; *see also id.* ¶ 70. Google then uses the data it intercepts for its own purposes. *See id.* ¶ 73 (In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.). Courts across the country recognize that companies cannot evade liability in circumstances like this. *See*, *e.g.*, *Robinson v. Disney Online*, 152 F. Supp. 3d 176, 182-83 (S.D.N.Y. 2015) ("[Defendant] could not disclose the information at issue here, along with a code that enabled [the relevant third party] to decrypt the hashed serial number and other information necessary to determine the specific user, and still evade liability."); *In re Hulu Priv. Litig.*, 86 F. Supp. 3d 1090, 1097 (N.D. Cal. 2015) ("No one would deny that I would violate the VPPA by passing someone an encrypted list of Judge Bork's video rentals—if my recipient and I both understood that we would use a mutually intelligible code."). This Court should do the same.

D. Google Intercepted the "Contents" of Plaintiffs' Communications With Their Healthcare Provider

Defendant argues that Plaintiffs' claims brought under the CIPA and WESCA should be dismissed because they have not alleged that Google intercepted the "contents" of their communications. MTD at 18-19. That is wrong.

CIPA § 631(a) prohibits the unauthorized disclosure of the contents of communications. Cal. Penal Code § 631(a). As used in § 631(a), "content" refers to the "intended message conveyed by the communication." *In re Meta Pixel Healthcare Litig.* ("*In re Meta Pixel*"), 647 F. Supp. 3d 778, 795 (N.D. Cal. 2022). "Analysis of CIPA violations is the same as the analysis for the federal Wiretap Act, … and [u]nder the Wiretap Act, 'contents' is defined as 'any information concerning the substance, purport, or meaning of [a] communication.'" *Byars v. Goodyear Tire & Rubber Co.*, 654 F. Supp. 3d 1020, 1027 (C.D. Cal. 2023) (internal citations omitted). "[C]ontent" includes "the names of buttons clicked," *see In re Meta Pixel*, 647 F. Supp. 3d at 795, along with "search queries" and "the particular document" requested. *See Brown v. Google LLC*, 2023 WL 5029899, at *15 (N.D. Cal. Aug. 7, 2023); *see also Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019) ("Revitch requested information from Moosejaw by clicking on items of interest; Moosejaw responded by supplying that information. This series of requests and responses – whether online or over the phone – is communication."). "Content" may also include "full-string, detailed URLs" that include "'the particular document within a website that a person views[.]'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 605 (9th Cir. 2020); *see also In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1083 (N.D. Cal. 2015) ("URLs (to the extent the URLs contain a user's search terms) implicate 'content' under the Wiretap Act.") (internal citations omitted).

Here, Plaintiffs allege that the contents of their communications were intercepted by Google. For example, when consumers, including Plaintiffs, purchased prescription medication for erectile dysfunction through BlueChew's Website, Google intercepted the contents of those communications. FAC Figures 8-9. Under California law, such information is the "content" of the communication, as opposed to mere record information, because it is the "intended message of the communication." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 795; *see also Revitch*, 2019 WL 5485330, at *1. The fact that such content was conveyed through an identifier recognizable by Google is of no consequence. Each of these interceptions is tethered a patient's PII, including their first and last name, email address, and date of birth, which Google uses for

identification purposes to direct its targeted advertising. FAC ¶¶ 68-73. Defendant's argument that such information is merely "record" information lacks merit.

E. Google Was Not a "Mere Vendor" to the Communications Between Plaintiffs and Their Healthcare Provider, It Was an Eavesdropper.

According to Defendant, Plaintiff M.D.'s CIPA Section 631 claim fails because Plaintiff only alleges that Defendant acted as a mere "vendor" to Blue Chew, and therefore Defendant could not have "intercepted" a communication. MTD at 19-20. Defendant further argues its "judicially noticeable policies and terms specifically show that data from certain types of websites" are "handled differently" and "not used for targeted advertising." *Id.* at 21. That is wrong.

First, the question of whether Defendant is a "vendor" or a third-party eavesdropper is a question of fact not suitable for determination on a motion to dismiss. *Kauffman v. Papa John's Int'l, Inc.*, 2024 WL 171363, at *7 (S.D. Cal. Jan. 12, 2024) ("Whether FullStory acts akin to a tape recorder or whether its actions are closer to 'an eavesdropper standing outside the door' is a question of fact which is better answered after discovery into the session replay technical context of the case."); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) ("The question thus becomes, in analogue terms: is Quantum Metric a tape recorder held by Lululemon, or is it an eavesdropper standing outside the door? This is a question of fact for a jury, best answered after discovery into the storage mechanics of Session Replay."); *Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934, 942 (S.D. Cal. 2024) ("The Court finds here that whether ASI acts akin to a tape recorder or whether its actions are closer to 'an eavesdropper standing outside the door' is a question of fact which is better answered after discovery.").

Second, both of Defendant's arguments are belied by the FAC. Specifically, Plaintiff alleges "[o]nce Google's software code collects the data, it packages the information and sends it to Google Analytics for processing." FAC ¶ 71. "After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages." *Id.* ¶ 72 (emphasis added). "In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users." *Id.* ¶ 73 (emphasis added). "As a

result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least 'Custom Events' and URLs that disclosed the name of the prescription medication and the medication quantity and dosage. Google also received additional PII, including first and last name, email address, and date of birth, that uniquely identify the patient, as shown below in Figures 8 and 9." *Id.* ¶ 75. Thus, "[w]hether or not a third-party service incapable of using the data it collects might avoid liability under Section 631, the complaint alleges that Google *does* read and use Google Analytics data." *Smith*, 735 F. Supp. 3d at 1197 (emphasis in original).

Against this backdrop, Defendant's argument that Plaintiff only alleges Google "function[s] as an extension of BlueChew" or that it collected data "for BlueChew's benefit only" holds no weight. MTD at 20, 21. Defendant's reliance on *Noom* and *Doe v. Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *17 (N.D. Cal. Apr. 11, 2024) is therefore unavailing because Plaintiff indeed alleges Google uses the collected information for its own purposes and benefit, notwithstanding its "policies and procedures." FAC ¶¶ 71-75. *See Smith*, 735 F. Supp. 3d at 1198 ("Plaintiffs' allegations, which must be taken as true, suggest that Google is not simply a vendor of a tool that websites can use to 'record' their own users' interactions on their websites, but rather that Google read or used the data collected about these users."); *see also id.* ("While Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited developers from transmitting such data, this presents a question of fact that the Court cannot resolve at this stage."); *Valenzuela v. Nationwide Mut. Ins. Co.*, 686 F. Supp. 3d 969, 980 (C.D. Cal. 2023) ("Eavesdropping on a conversation at the time it occurs is a violation of Section 631, even if done for the benefit of a party to the conversation.").

F. Plaintiff M.D. States a Claim for Invasion of Privacy under the California Constitution.

1. Plaintiff M.D. has a reasonable expectation of privacy in his purchase of erectile dysfunction medication.

To state a claim for invasion of privacy under the California Constitution, Plaintiff "must show that (1) [he] possess[es] a legally protected privacy interest, (2) [he] maintain[s] a reasonable expectation of privacy, and (3) the intrusion is 'so serious ... as to constitute an egregious breach of

the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)).

Defendant first argues that "Plaintiff M.D. lacked a reasonable expectation of privacy" in the seeking and purchase of erectile dysfunction medication. MTD at 22. This argument defies logic and, to no surprise, has been rejected numerous times by courts throughout this District and Circuit. *See, e.g.*, *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 800 (N.D. Cal. 2022) (denying motion to dismiss, holding the plaintiffs "will likely be able to show that they had an objectively reasonable expectation that their communications with their medical providers"); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 603 (finding an objectively reasonable expectation of privacy existed where plaintiffs plausibly alleged that Facebook did not disclose that the information at issue would be collected).

Next, Defendant claims "[v]isitng BlueChew and completing a profile does not indicate that Plaintiff M.D., or any individual, has any medical condition at all." MTD at 22. But Defendant overlooks Plaintiff M.D.'s allegation that "[a]s shown in Figure 9, Google is intercepting information related to patients' prescription medications." FAC ¶ 69. Thus, the allegations go beyond Google's interception of information pertaining to completion of a Blue Chew profile. Google also intercepts purchase information of prescription erectile dysfunction mediation.

Defendant further argues Plaintiff M.D. "lacks a reasonable expectation of privacy in the pseudonymous identifier created by BlueChew to denote a particular medication and dosage[.]" MTD at 23. To the contrary, however, Plaintiff has a reasonable expectation of privacy in the fact that he purchased erectile dysfunction medication—which Google intercepted—along with Plaintiff's personally identifiable information. That is sufficient. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 801 ("Meta does not point to a single case where a court found that the collection of the kinds of information at issue here did not constitute a highly offensive invasion of privacy."); *St. Aubin v. Carbon Health Techs., Inc.*, 2024 WL 4369675, at *12 (N.D. Cal. Oct. 1, 2024) ("As Plaintiff has alleged, the URLs pertain to appointments the Plaintiff made, and the transmitted URLs

contain information regarding the specific symptoms, physical condition, or course of treatment of an individual. … The pleadings here are sufficient to support a reasonable expectation of privacy.").

2. Defendant's interception of information pertaining to the purchase of erectile dysfunction medication is highly offensive.

Defendant argues Plaintiff M.D. cannot establish its intrusion was an egregious breach of social norms because, according to Defendant, "Plaintiff alleges that Google collected his name, birthday, and email address." MTD at 23. Here too, this ignores the allegation that Defendant intercepts information pertaining to Plaintiff's purchase of erectile dysfunction medication, including "the type of medication being purchased by patients" in addition to "the quantity and dosage." FAC ¶¶ 69-70.

Defendant's conduct was highly offensive. As an initial matter, "questions of whether conduct is 'egregious,' 'offensive,' or violates 'social norms' tend by their very nature to be subjective . . . [and] these questions are typically more appropriately resolved by a jury." *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1139 (E.D. Cal. 2021); *see also In re Google Location Hist. Litig.*, 514 F. Supp. 3d 1147, 1157 (N.D. Cal. 2021) ("Whether [defendant's] collection and storage of location data when Location History was set to off was highly offensive to a reasonable person is a question of fact.") (citing *Facebook Internet Tracking*, 956 F.3d at 606). Indeed, the Ninth Circuit held that this determination "requires a holistic consideration of factors" and raises "an issue that cannot be resolved at the pleading stage." *Facebook Internet Tracking*, 956 F.3d at 606.

Here, Plaintiff M.D. has identified sufficient facts to survive a motion to dismiss because he pleads that Defendant surreptitiously collected his private health information in unexpected ways. Indeed, under similar circumstances, the court in *In re Meta Pixel Healthcare Litig.* found:

> There is support for plaintiffs' position that Meta has behaved egregiously. By enacting criminal and civil statutes forbidding the disclosure of protected health information without proper authorization, Congress has made policy decisions regarding the importance of safekeeping this information. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information). Courts have also found that taking personal contact information without consent could be deemed highly

> offensive. *See Opperman v. Path*, 87 F. Supp. 3d 1018, 1060–61 (N.D. Cal. 2014) (finding that a jury must decide whether the "surreptitious theft of personal contact information" is highly offensive). Finally, I note that Meta's policies forbid the transmission of health-related information, which the Ninth Circuit has found to be relevant in the "highly offensive" inquiry. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 606 (finding that highly offensive element was sufficiently pleaded where Facebook collected full-string detailed URLs and where "Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue."). These arguments have merit.

647 F. Supp. 3d at 800-01; *see also M.G.*, 2024 WL 4219992, at *6 (Martínez-Olguín, J.) (egregious nature of similar conduct raises "a factual dispute and Headway has not met its burden to show that the information disclosed here – M.G.'s provider preference, appointment details, and search concerning mental health conditions – cannot allege a serious invasion of privacy").

The same analysis applies here. Defendant's conduct in surreptitiously intercepting Plaintiff M.D.'s private health information—pertaining to the purchase of erectile dysfunction medication—to use for its own advertising purposes is highly offensive. At minimum, a reasonable jury could conclude that it is highly offensive. Therefore, Defendant's motion to dismiss Plaintiff M.D.'s claim of invasion of privacy under California's Constitution should be denied. *See R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 893 (C.D. Cal. 2024) ("The SAC explains how Defendant's disclosure of their private information to Meta via the Pixel included the purchasing of sensitive healthcare products (Monistat and a diabetes test kit) related to specific health conditions (yeast infection and diabetes). … The Court finds those facts sufficient to survive a motion to dismiss based on the 'highly offensive' element."); *St. Aubin*, 2024 WL 4369675, at *13 ("Second, Plaintiff contends that the disclosure here is highly offensive because it involves Plaintiff's medical information. This Court agrees with other courts that have refused to dismiss invasion of privacy claims at the motion to dismiss stage where, as here, a data breach involved medical information, because the disclosure of such information is more likely to constitute an 'egregious breach of the social norms' that is 'highly offensive.'") (citing *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1143 (C.D. Cal. 2021)).

Last, Defendant argues "an egregious breach cannot exist because Google required BlueChew to disclose BlueChew's use of Google Analytics, BlueChew did so, and Plaintiff M.D. consented to such use." MTD at 24. Plaintiff M.D. did not consent to the disclosure of his purchase of erectile dysfunction medication to third parties for the reasons explained *supra*, Section III.A.

IV. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court deny Defendant's Motion to Dismiss. If the even the Court concludes that any portion of Plaintiffs' FAC is deficient, Plaintiffs seek leave to cure any such deficiencies.

Dated: April 7, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiffs